*International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868*
*Foundation of Computer Science FCS, New York, USA*
*Volume 12– No.32, August 2020 – www.ijais.org*

# Biometry, Encryption and Spyware (BES): A Multi-factor Security and Authentication Mechanism for JAMB E-Examination

Amadi Rapheal Sunday
Department of Cyber Security Science
Federal University of Technology
Minna, Niger State, Nigeria

Ismaila Idris
Department of Cyber Security Science
Federal University of Technology
Niger State, Minna, Nigeria

Hussaini Abubakar Zubairu
Department of Information and Media Technology
Federal University of Technology
Minna, Niger State, Nigeria

Stella Oluyemi Etuk
Department of Information and Media Technology
Federal University of Technology
Minna, Niger State, Nigeria

Idris Mohammed Kolo
Computer Science Department
Federal University of Technology
Minna, Niger State, Nigeria

## ABSTRACT
Electronic examination is the innovation of assessing students electronically. In recent times, it has gain popularity and acceptance. The gradual acceptance and popularity of electronic examination was underscored by its benefits. However, e-examination security has been considered a major challenge in e-learning, in which malpractices-free e-examination seems elusive. Collusion, online assistance, surfing the Internet and remote sharing of desktop are security threat to the current JAMB's e-examination. This paper proposes an e-exam system using a multi-factor security and authentication mechanism. Biometry, Encryption and Spyware (BES) are adopted to enhance security and authentication of JAMB's electronic examination. Biometrics are used for authentication, Encryption for the security of the data and the databases and Spyware for e-monitoring. The proposed system addresses the security and authentication lapses of the existing JAMB's online examination. Evaluation of the system was performed in term of impersonation, accessing the Internet or remote sharing of desktop to assess the security and authentication effectiveness of the proposed system. The evaluation shows a promising results towards addressing authentication and security issues in the JAMB's online e-exam.

## General Terms
Security, authentication and e-Exam

## Keywords
Electronic examination; biometric, security, encryption, spyware, JAMB.

## 1. INTRODUCTION
Online or electronic examination is becoming more acceptable and popular following the increased use of the internet or intranet and students can now take their examination using any IT facilities that is internet or intranet enabled [7]. Online examination is a virtualize form of an examination using digital medium such as Internet or Intranet on Local Area Network (LAN) [24]. The World is going digital and everything is done at the click of mouse, due to the availability of World Wide Web (Web) and the Internet. The Information Communication Technology (ICT) is adding value to the learning processes and to the organization and administration of learning institutions. In addition, [19] believes as a result of advances in ICT, many academic institutions are now using online delivery of assessment, and as a result, e-assessment has increased for both formative and summative purposes.

ICT focuses on the application of new technologies in an educational context and environment, and serves as a tool for supporting the various components of education. One specific application of ICT is the Computer-Based Testing (CBT), also known as Computer-Based Assessment or Electronic Examination. It is a method of administering tests in which the responses are electronically recorded, assessed, or both. It is commonly available for several admissions tests throughout the developed countries [9]. More recently, variously electronic assessment designs have been worked on by researchers, this can considerable impact the learning progress of the students [4].

The present electronic examination that is highly applauded is aim at replacing the traditional paper and pencil mode of writing examination [15], which has been widely criticized because of various frauds that has characterized the process [16].

In Nigeria, there exist various examination bodies such as Joint Admission and Matriculation Board (JAMB), West Africa Examination Council (WAEC), National Examination Council (NECO), National Board for Technical Education (NABTEB), National Teacher Institute (NTI). These examination bodies are key-in to the idea of electronic examination. JAMB, an examination body that is responsible for conducting an entrance examination to the Nigerian university has introduced the online examination for student seeking for an admission into tertiary institutions in Nigeria [16].

However, as Information Technology and Internet mature and online examination is becoming the mainstream of an assessment in academics or education, many issues have emerged [5]. It has also become an avenue for several illegal activities [11]. The advancement of the Internet and web has given rise to the popularity of online examination, but Security of the process remains a serious challenge. The security requirements for the JAMB e-examination is the use of password. The JAMB administrator authenticates the candidates using fingerprint registered with the examination body during registration. Prevention of fraudulent activities is performed using security agents and the use of webcam as proctor. This paper aims at overcoming security and authentication-related problems in JAMB online examination system with a multi-factor based security and authentication scheme (BES).

This paper propose the authentication of the students using password and biometrics (fingerprint and facial recognition). They address the issues of the integrity of the exam through the use of cryptography scheme for the encryption of both the question and the candidate's biometrics. Prevention against the use of messaging applications, surfing the Internet and remote desktop sharing during was achieved using spyware for e-monitoring.

## 2. PROBLEM DEFINITION

The electronic or computer based examination is currently gaining acceptance as an easy means of conducting an examination. As a consequence of the popularity of the computer and its effectiveness and efficiency, hundreds of thousands of examination bodies and Higher Institutions are trying to migrate to computer based examination, with National Open University Nigeria (NOUN) being the first to conduct an electronic examination in Nigeria [16]. As the electronic examination continues to gain acceptance and popularity, the convenience associated with electronic examination will attract more institutions and examination bodies. One expectation of electronic examination is that it will replace the traditional pencil and paper form of examination [10].

While electronic examination is increasing gaining acceptance, as a result of information technology and web, the security of e-examination remains an issue [15]. To maintain quality, integrity and trust in e-examination and in long term the educational process itself, it is vital that security is strong. Thus, it can be helpful to reduce opportunities for cheating and put mechanism in place to thwart any chance of student to cheat in an electronic examination.

The security issues related to e-examinations include unauthorized access, impersonation and modification of the questions at the database level. Swapping of answers, surfing the internet for solution, or using the resources on the local computer (data or software) are other security lapses that that could be envisage in an e-examination [15].

Typically, most examination bodies do not have enough physical facilities for all students so they have to rely on higher institutions with e-examinations centres in order to allow students to hold their examinations. Therefore, exam management becomes more complex since such external e-examination centres must be provided with all management mechanism to ensure that students will be able to have their examination in a desired location. The current e-examination process adopt by JAMB is prone to modification, impersonation, doctrine and remote desktop sharing Thus, there is need for effective security and authentication mechanism to ensure the security and integrity of the process.

## 3. LITERATURE REVIEW

### 3.1 Existing Architectures of E-Examination

According to [25], in the e-examination environment, the examination data is delivered electronically to students who may-be remotely connected through a computer network (i.e. internet/intranet). In most scenarios, the examination body (i.e. examination centers) and data resides in entirely different geographical locations and are connected via the internet. In Nigeria, and also in the world at large, the architecture or model of the process is almost the same. The architecture of the existing electronic examination systems according to [2], is represented in figure 1 below.

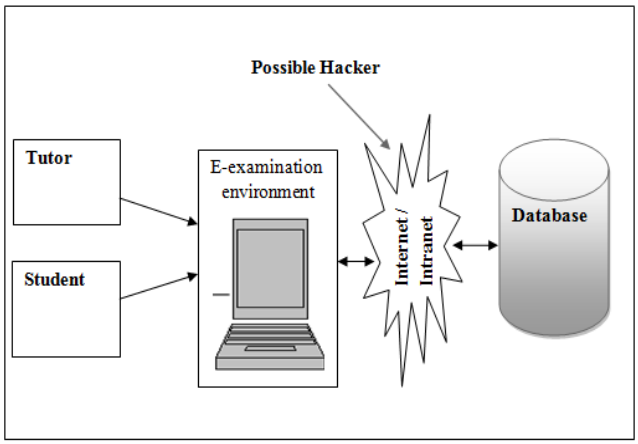


**Figure 1: The existing e-examination architecture [2]**

The examination body is responsible for the preparation of the e-examination questions by asking those in charge to submit the questions to the database administrator at the center. The database administrator uploads the questions into the database at the examination body's server. From the examination body database, the questions are upload into the internet (cloud server) for various testing centers to download it into their local servers some few hours to the commencement of the examination.

The e-examination systems can be accessed by both students and tutors (i.e. educators) who are located remotely. The databases which contain all the required information are stored in servers at any location, as per the requirement, by the educators. Once the student gives a request to access the required information, the databases in the servers are accessed through the web server. The students have facilities to access documents/files uploaded by the educator, provided the student has sufficient authentication privileges as shown figure 2

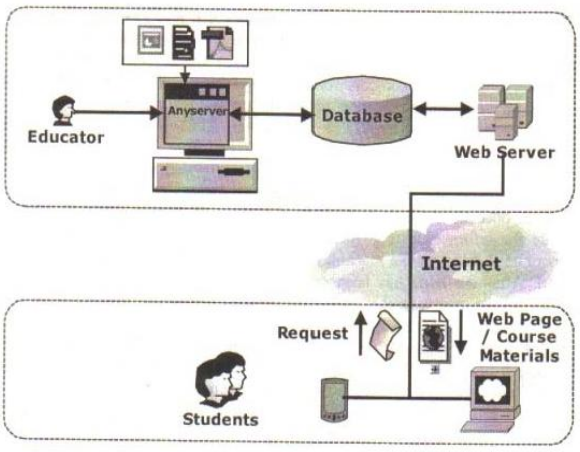


**Figure 2: E-examination Systems Component Diagram [3]**

The implication here is that, when examination data (i.e. questions) passes through so many hands it is likely that the integrity of the questions may be compromise, especially when a private individual is involved.

The architecture of e-examination depicted in figures 1 and 2 above are adopted by virtually all e-examination systems with only little variation or modification. This type of architecture did not give security issues too much attention especially social engineering, remote sharing and instant messages. The biggest potential security problem in e-examination setting is of human, rather than electronic origin. The weakest link in any security system are the people using it.

## 3.2 Related works

[17] Design and developed an online examination system that uses the examinee's biometrics to authenticate the identity of the examinee. The student's fingerprint is used as login credentials into the examination system. Though, this system is better than the traditional password based online examination system. But, the system does not address the issue of forbidden stuff and an accomplice. Cheating and malpractices is still possible with this system.

[20] Designed an e-examination system that integrates a webcam to capture audio and video. The video footages are extracted and the yaw angle variations are calculated and audio input is compared with a certain predetermine threshold value. From the footage of video and audio analysis, it could be determining whether a candidate has indulged in examination malpractice or not. The computational complexity of this system make it practicality very limited. In addition, monitoring of images of every candidates taking online exam by the proctor is not in all cases practicable. It causes additional overhead of network and storage issues.

[6] Maintain that manual examination system faces problems of result processing, filing, tendency of losing records and difficult in searching for record. Consequently, they proposed an online examination system that is internet based. The aim was to make examination effective, efficient and cut down the amount resource usage. The security challenges associate with online examination was not address in this system. There is no measure put in place to checkmate the security vulnerability in the proposed system. It does not provide any method to prevent malpractices. The system can be enhanced by encrypting the question and randomization of questions to reduce the level of examination malpractice.

[1] Designed an e-Exam system that was implemented on client-server network architecture on few computer laboratories at the department of Information Technology in Lebanese French University. The system is used in the institution for class quizzes, midterm and final examination to replace most of the paper based examinations in the institution. A customize browser was used for the implementation of the system using C# (C Sharp). Though, it was reported to have perform relative better, the architecture does not take adequate need of all the components in the system, the security of the database-an essential component of the system is still vulnerable as anyone who has an authenticated access can also break the database and copy the contents from the database. The focus of the research was to automate the conventional paper and pencil based examination system. The password based nature of the system is not sufficient to prevent malpractices.

[21] Address the security challenges in e-examination by proposing a continuous authentication approach. The security mechanism implemented in their proposed e-examination system involves the combination of facial recognition, mouse dynamics, and keystroke dynamics. These modalities are collected and processed during the exam without requiring any predefined actions from the candidate. While these might help to prevent cheating to some extent, the drawback is that the continuous surveillance might cause uneasiness to the candidate, the use of Keystroke pattern has low accuracy and permanence since the user typing pattern might change with an improvement in typing skill.

[13] Propose a web based online examination using Java Web technologies. The system has the capabilities of question administration and quiz generation. The potential benefit of the mix of customer side programming and server-side programming methods were used and analyzed. Essentially, this system only implements randomization of question to mitigate the level of malpractice. Even though, there is no evaluation of the system, the major drawback of the system is that impersonation is still very possible since verification is manually done.

[10] Highlight the security challenges of e-examination, such as integrity and impersonation. To address these challenges, they developed a desktop application using Java Programming language. The system integrates fingerprint authentication, image capturing and data encryption for effective security of the system. While this system solves some security issue, it performance in terms of security and integrity of the system is far from being adequate. The authors did not take cognizance of the insecure channels of transmission. Though, the data was encrypted but if the network is not secured, is just a question of time, the encryption can be broken.

[15] developed an examination system that adopt the use of a face-recognition system, one-time password (OTP) generation and a fingerprint mechanism to enhance the security of the online examination systems. OTP can be sent through mobile device and cheating can occur in an online examination without the movement of face, especially when accessing the system resource or seeking assistance online.

[18] adopt the methodology of research design to developed a secure computer based testing systems for tertiary institutions with an embedded fingerprint to provides an improved means to protect examination question against unauthorized access. The system was developed using HTML, PHP, MySQL and JavaScript. Evaluation of the system was carried out on a

local server using WAMP server and was adjudges effective in improving the integrity of the e-examination. Although a biometric technology is used, which is better compare to usernames or passwords, but authentication only happen at login time. Thus, not enough to prevent cheating from occurring during the course of the online examination.

[11] Propose an online examination system that performs automatic verification of candidates' identity vie the server. A simple authentication dialogue was created for completion of the authentication to be done between the student and the server. The system securely manages distribution and collection of papers and answers respectively. While this approach might work for limited scenario, the restricted nature of these approaches might be a serious drawback in real-world implementation.

Most of these review works adopted the use of what you know, who you are, challenge question, encryption, webcam, mouse dynamics and keystroke for security and authentication. However, most of these research did not give much attention to collusion, abetting, impersonation and remote desktop Sharing. Though PC lockdown or secure browser was implemented in some research [14] [22] to minimize the chance of student using messaging applications, application switching, surfing the Internet or desktop sharing during an examination [12], it is still possible for a student to engage in malpractices, accessing the internet or resources from the local system and share information with a third party. These area has not been given much attention in the previous research and the existing JAMB e-examination is prone to these vulnerabilities. This paper proposed a multi-security and authentication e-exam system to enhance the security and authentication process of the JAMB e-exam. They propose a BES security mechanism to address the security vulnerabilities of e-exam highlighted by [23].

Biometrics (fingerprint and facial recognition). Fingerprint and facial recognition for authentication against impersonation, Encryption of the questions to ensure its integrity during storage, transportation and processing, and Spyware to monitor the activities of candidates against messaging applications, surfing the Internet and remote desktop sharing during an examination.

## 4. METHODOLOGY

We conducted vulnerability assessment of the JAMB e-exam at five different testing centers currently used by JAMB to conduct electronic examination in terms of the security vulnerability outlined in [23]. The process flow chart for the existing systems is presented in Figure 3.

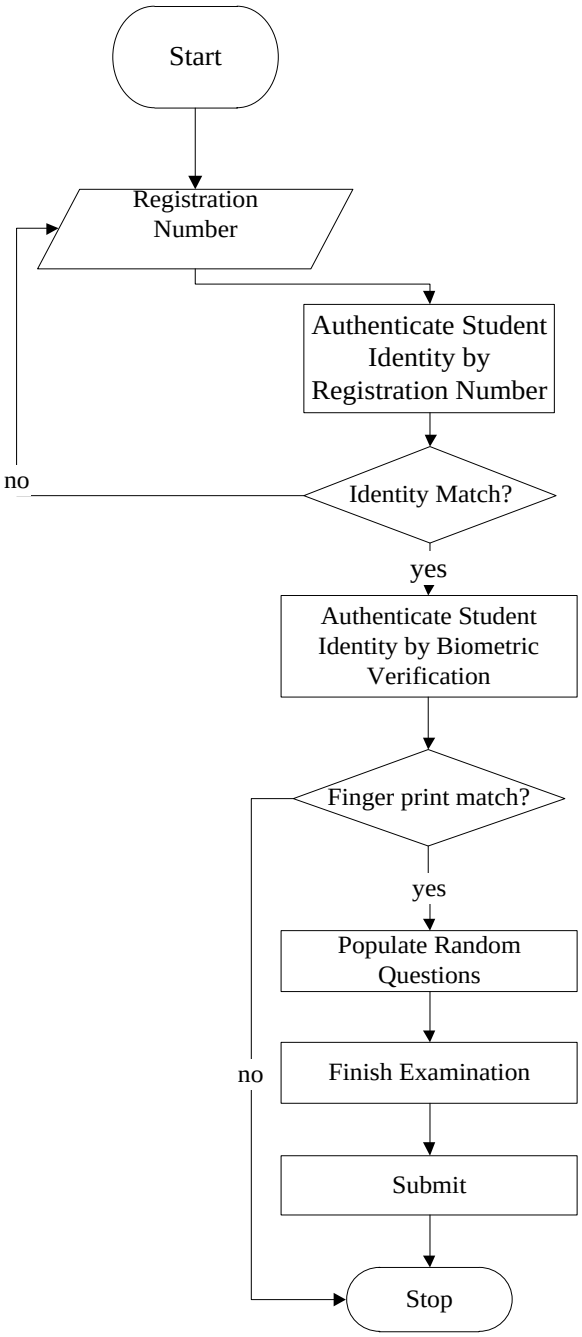


**Figure 3: The existing system process flow chart**

The process flow chart presented above does not give much consideration to the security vulnerability of e-examination, as such creating room for security vulnerabilities discussed in [23]. Consequently, object-oriented analysis approach was adopted to develop a multi-security and authentication e-exam system using Java Programming Language. The proposed architecture is shown in figure 4. The components of the architecture are: The test center that contains the students PC, the Internet (cloud server), the security layer (the organization intranet) and the database components.

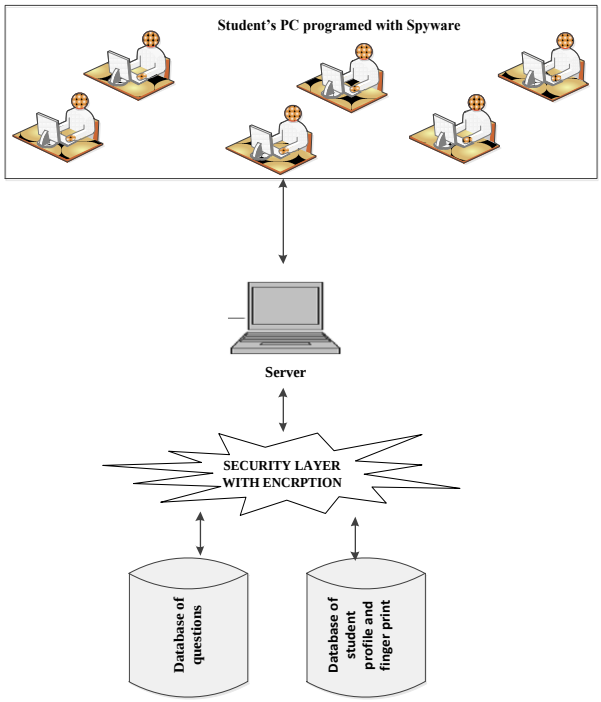


**Figure 4: The proposed E-examination architecture**

**A.** The Test Center

The test centers host the student's personal computer (PC). This can be viewed as a work station that host several computers or systems. Monitoring e-examination as in the conventional paper and pencil examination is not feasible, they envisage a time to come where the students are expected to take not just multiple choice questions but are expected to key in value in to the system, therefore PC lockdown or secure browser as currently used as security measure will no longer be applicable. Therefore, it is necessary for JAMB e-examination system to have some remote monitoring system to prevent and to detect cheating. Therefore, every student's PC, in addition to an inbuilt webcam have programmed spyware. The spyware functionality is to register and log all activity that can later be analyzed to determine if any form of examination malpractice has taking place during the examination. This module is programmed to log out any student that attempt to initiate messaging, access some prohibited resources or internet. This scheme relies on the fact that there can still be a forbidden action after the examination questions might have been decrypted by the student, which cannot be detected by an inbuilt webcam or the physical presence of supervisor or an invigilator.

**B.** The Security Layer

The security layer of the architecture is responsible for IP address Security. This layer was implemented as a firewall to check for the security breaches in the databases that are wrapped up into a single unit. Each access may have to satisfy certain security constraints before granting an access to any information in the databases. All traffic from inside to outside, and vice versa, must pass through the security layer for screening. Only authorized traffic, as defined by the security policy of the system, will be allowed to pass. The security layer itself is designed to resist penetration. This implies the use of a trusted system with a secure operating system. The security layer is designed such that an attacker would find it difficult to break or have an access to the databases.

**C.** Databases Components

The database component of the system stores both the question and the students profile along with their biometrics details. The entire information in the databases are encrypted. The student's database profile is encrypted to guide against manipulation. The question's database also uses cryptography mechanism for protecting questions in order to achieve the desired security levels at every exam stage. The questions are encrypted using Reverse Engineering Algorithm (REA) all through the transition until it gets to the students. The system was designed in such a way that the students fingerprint is tactically manipulated to serve as key to decrypt the question. The flow chart of the propose e-examination system is shown in figure 5. The dataflow diagram (DFD) and the activity diagram are shown in figure 6 and 7, respectively.

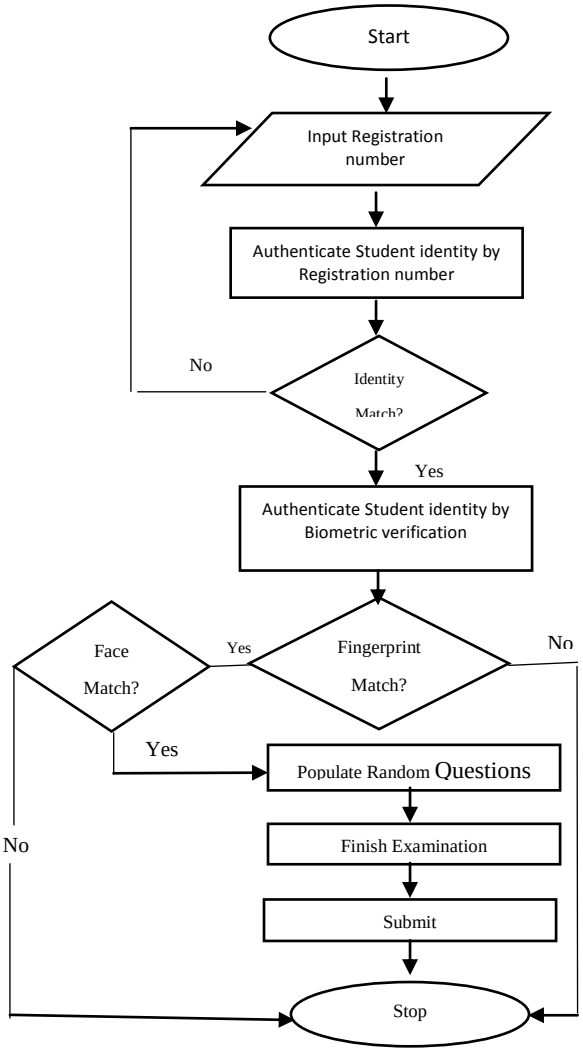


**Figure 5: The flow chart of the propose e-examination system**

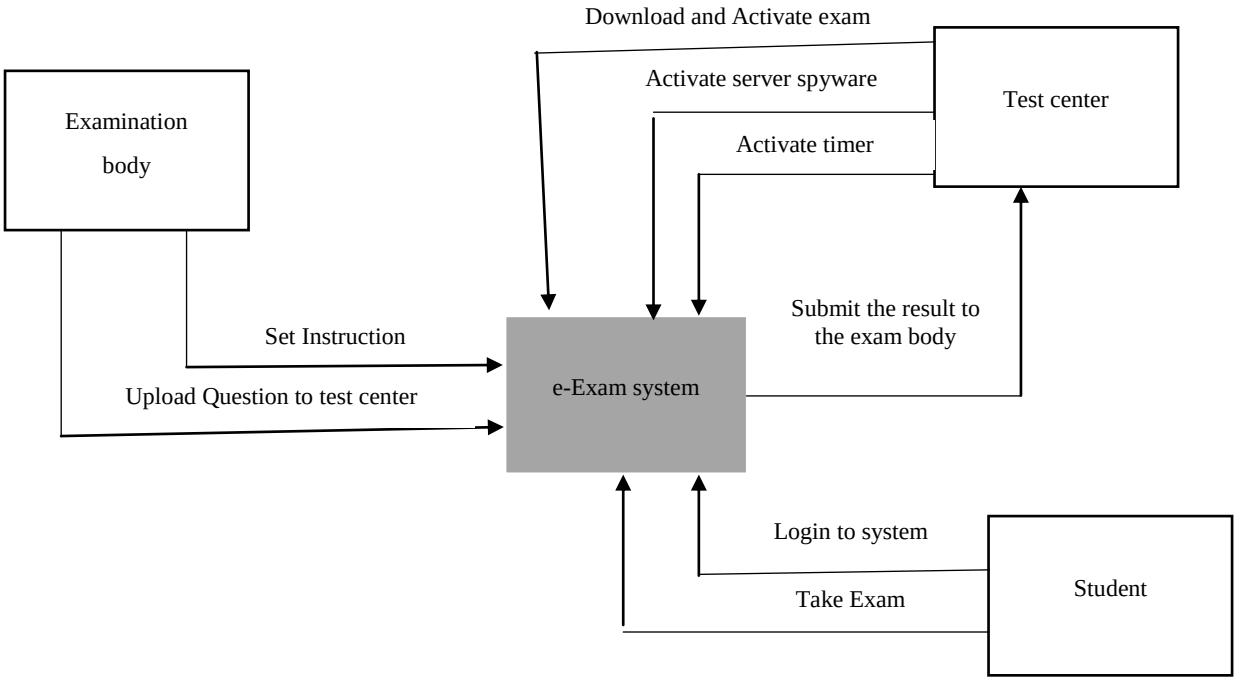


**Figure 6: Dataflow Diagram (DFD)**

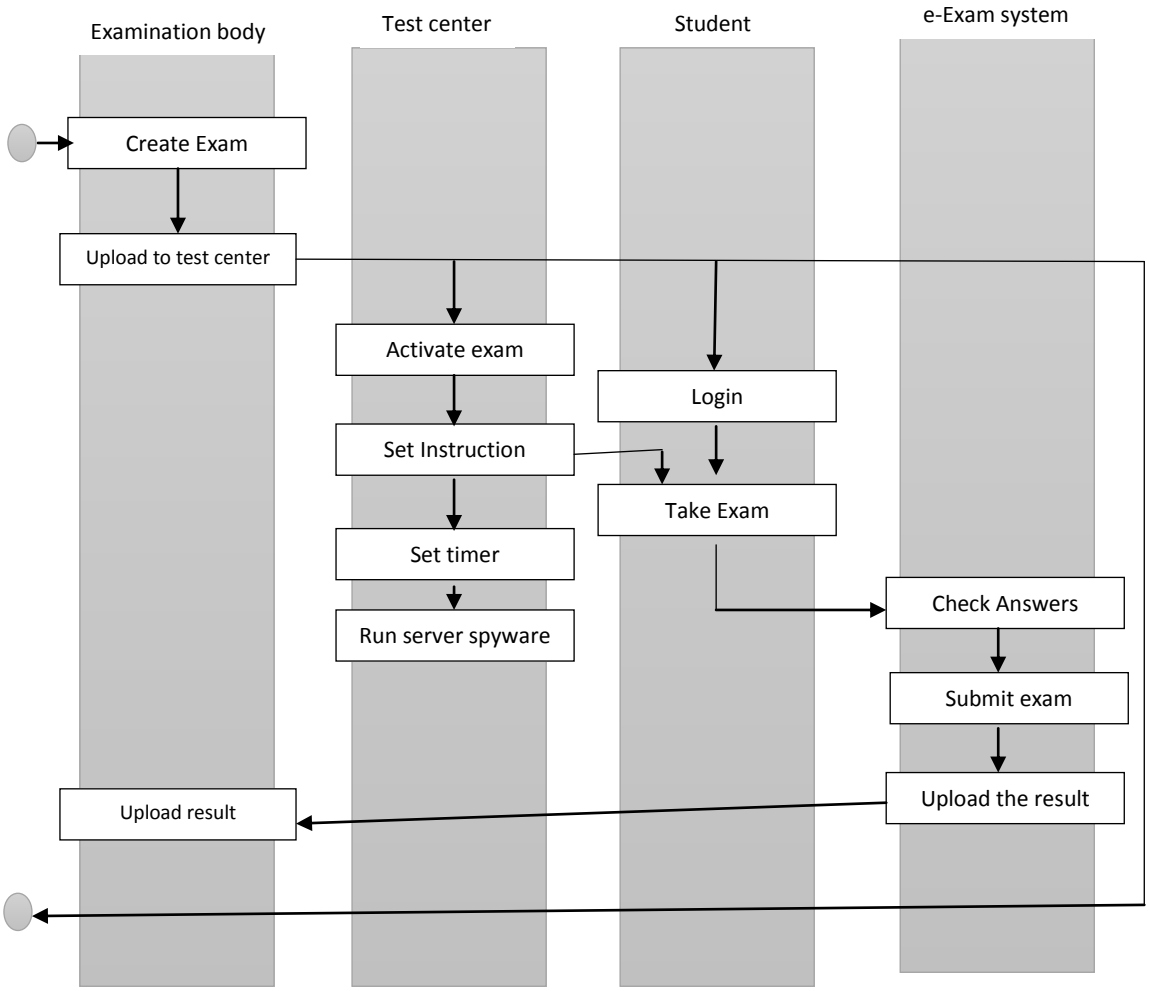


**Figure 7: Activity Diagram**

## 5. RESULT AND DISCUSSION

The system was implementation on the Intranet as shown in figure 8. In this approach, for stealthy electronic monitoring a student system must be connected to the Proctor's system (Administrator) through the Intranet/Internet as the case may be. The Administrator system creates a channel for each student to broadcast the exam session to his proctor through the portal of an examination server. Each candidate's session are monitored by the spyware through his/her channel, and all the sessions appeared on the proctor's terminal.

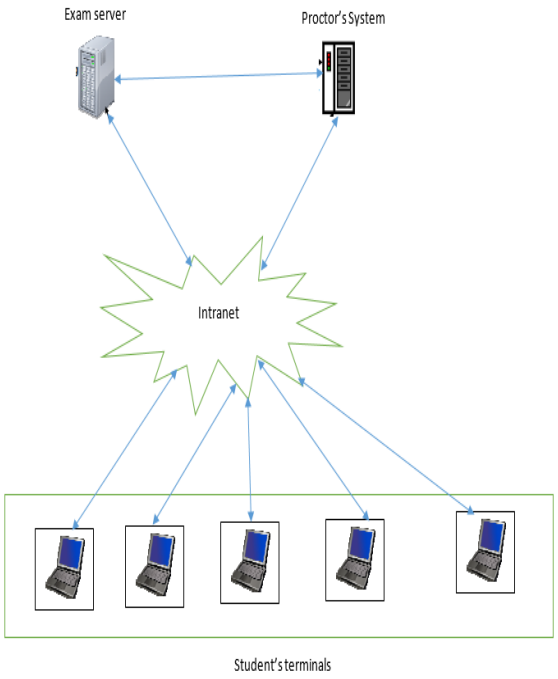


**Figure 8: The Intranet model for Spyware**

The testing and implementation of the system was carried out with five (5) number of system running on a server driven environment. The experimental setup was as depicted in figure 6 above. All the computers that was used have the following configuration; 2GB RAM, and 1.83 GHz Intel Core2Duo processor. The database server was PhpMyadmin. The system outputs are display below:

The main screen shots for the proposed e-examination system which was developed using java programming language is shown in figure 9 through to figure 17.

This screen provides two main options to perform the following:

(i) To enter the registration number of the student

(ii) To login into the e-examination application database.

This page is accessed and executed by the candidates. The candidates are required to fill in their registration number in order to login into the system. The access is granted only if the registration number is valid. The login form is display in figure 9. The use of registration number to authenticate students is not reliable, as students easily bypass it. In other words, impersonation is still recorded at some e-examination centers. Taking this into cognizance, there is additional security layer implemented in the proposed system.

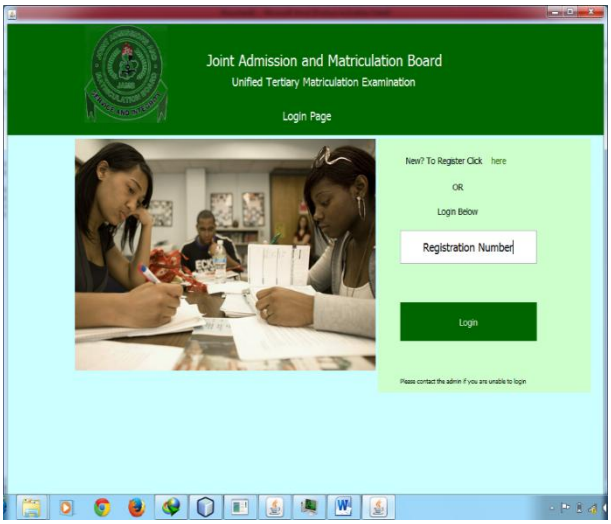


**Figure 9: Screen shot of the student login page**

If the student is logged on successfully, he or she is require to thumb print after clicking on proceed button in order to continue as shown in figure 10. With this feature integrated, it will be difficult to write an examination on behalf of somebody.

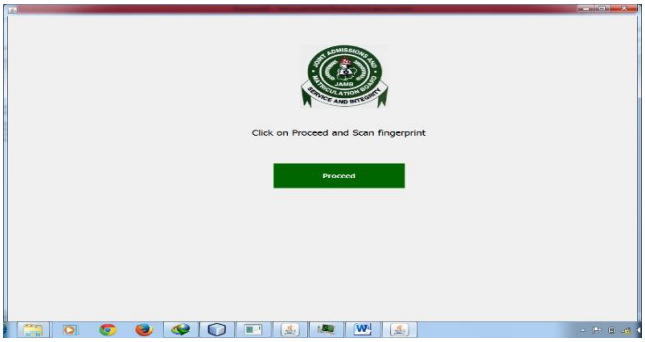


**Figure 10: Screen shot of finger scanning.**

If the finger print is detected, the system notified the student by displaying the screen shot in figure 11. And if the fingerprint is verified and a match was detected, messages will be display as show on figure 12.

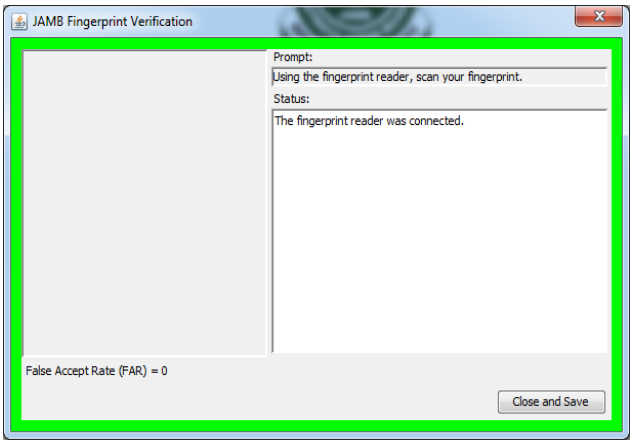


**Figure 11: Screen shot showing scanner status**

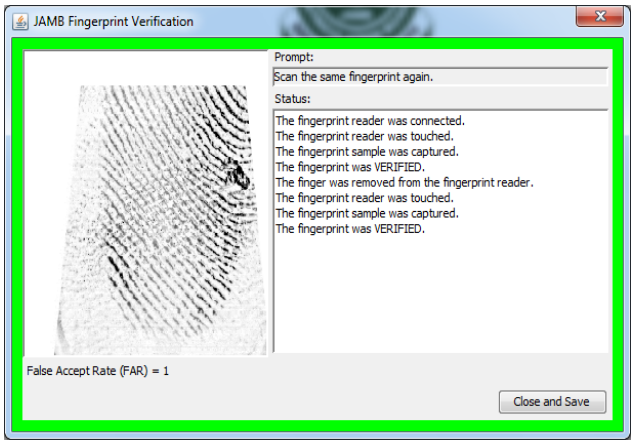


**Figure 12: Screen shot showing fingerprint verified**

If however the finger print does not match, error messages will be display as show on figure 13.

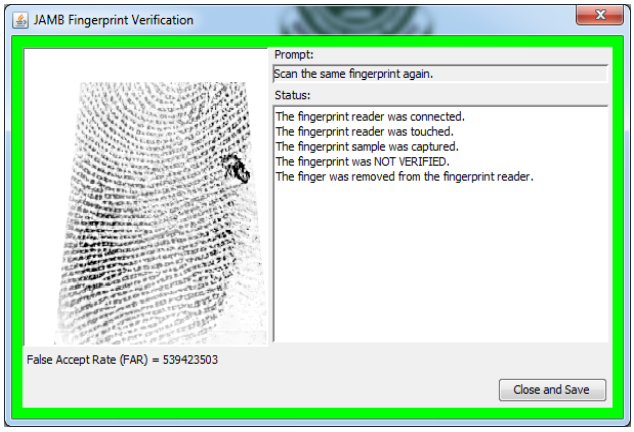


**Figure 13: Screen shot of fingerprint mismatch**

If the finger prints matches the registration number, the student is logged on to where he or she can see the subject combinations as shown in figure 14.

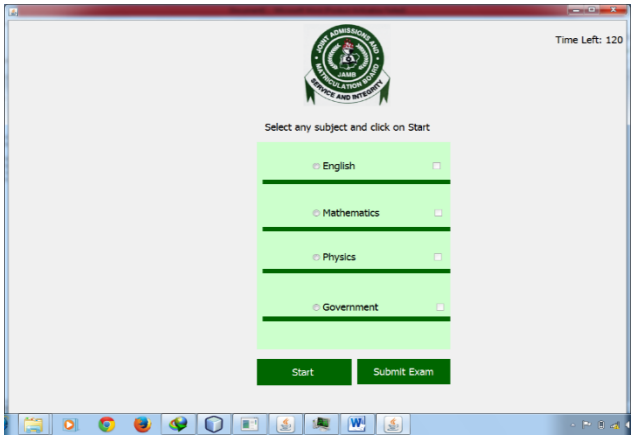


**Figure 14: Screen shot of subject combination**

In addition to the encryption of the question at the database level, the system is embedded with spyware that monitor all the systems and keep track of the session and activities. The active systems on the network and their corresponding IP addresses as the system was test run is shown in figure 15.

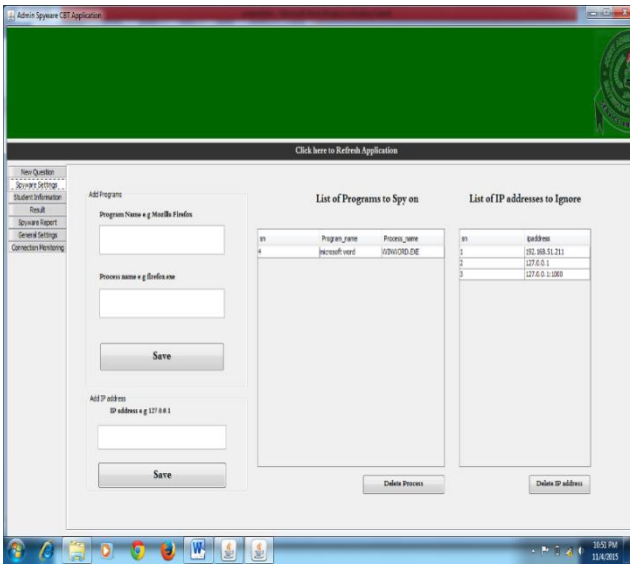


**Figure 15 : Screen shot of the systems running and their IP addresses**

Unlike the current practice, where the screen is locked as students take examination, instead the proposed e-examination allow the student to utilize all the system resources that are permissible but implement measures to log the student out of session if he or she tries to access the restrict resources like trying to access the internet or other computer resources restricted. Screen 16 shows the sample of student that was logged out of session.

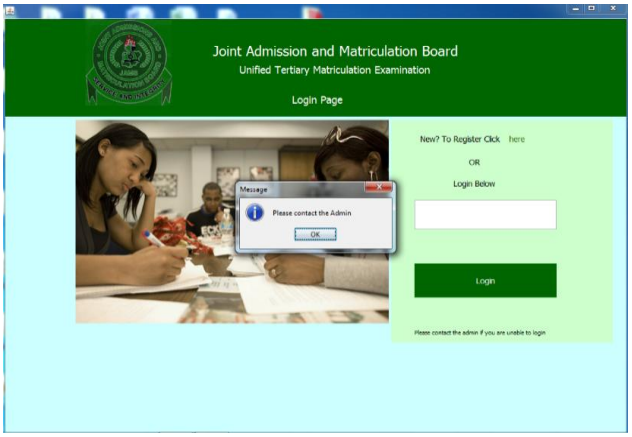


**Figure 16: Screen shot of logged out student**

This functionality was implemented in a module called Spyware report, the function of the module among other things is for monitoring and controlling calls made by applications and services. It was programmed to listen to specific IP address and API calls, such as file events, application events and Internet activity. During the execution of the spyware program, API Monitor displays intercepted API calls. For example application running activity is registered by the spyware program when the student opens any application.

These logs can be called later for analysis if there is any case of examination malpractices. Screen shot of spyware report is shown on figure 17.

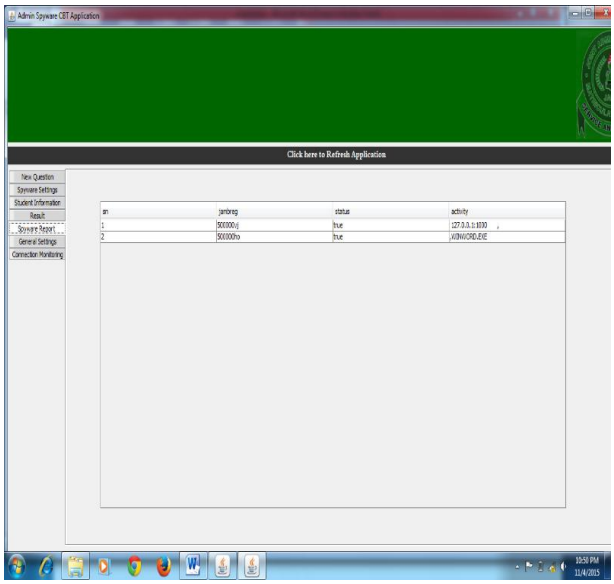


**Figure 17 : Screen shot of spyware report**

## 6. SYSTEM EVALUATION

Compared with the existing system, the implemented system has been evaluated in terms of different security breaches, impersonation threats and other cheating cases common in electronic examination according to (Frank, 2010). The implemented system has not been able to solve the issue of an accomplice and that of social engineering, but the system was able to prevents cheating scenarios of impersonation. The continuous monitoring and authentication is a major feature of the implemented system which is completely absent in the existing JAMB electronic system. Thus, it addresses the issues of instant messages, checking resources from the system, surfing the internet for answers and sharing of desktop.

Compared with the existing JAMB online exam system, it can be argued that the implemented system is reliable, secure and can increase the integrity of the JAMB e-examination, though requires more features and human intrusion to be deployed in large scale. Table 1 compare some features of the implemented system with the existing operated by the JAMB examination board.

**Table 1: Comparison of existing and implemented system in terms of different features**

| Features | Existing System | Implemented System |
|---|---|---|
| Application detection | Non | Functional |
| Keyboard and mouse logging | Non | Semi-functional |
| Process logging | Non | Functional |
| Impersonation | Still possible | Impossible |
| Virtual machine detection | Non | Not fully develop |

## 7. CONCLUSION

Electronic examination has gained popularity over the years. The benefits it offers has translate to the increase in the number of examination bodies that are adopting it as their mode of conducting an assessment. The acceptability of e-examination is on the increase and the Internet/Intranet is the major medium. However, the Internet is less secure, which therefore expose e-examination to security breaches and threats. Ensuring the security and integrity of e-examination requires that countermeasures be put in place.

This paper presents a secure electronic examination management system using security mechanisms such as encryption, biometric authentication and spyware tools. Every stage involves in e-examination and their security flaws have been identified and the different security features that every examination stage must satisfy to counter the security flaws inherent in the process have been clearly understood. Such information has allowed us to design and implemented a system based on different security protocols that offer a high security level for all e-examination stages.

In addition to the security vulnerability of the existing system, it was discovered that, there is no functional spyware to monitor the candidates as they take their examination, thus cheating can go unnoticed. All these security vulnerabilities of the existing system have been address by the new developed system.

The combination of spyware, biometrics and cryptography security mechanism proposed and implemented in this paper will provide and enhance security and integrity for JAMB online examination

Furthermore, the proposed system assumes that the test centre management and all those involve in the conduct of examination are honest; however, experience has shown that most of the cheatings perpetrated are orchestrated by social engineering. Further research should be directed to checkmate this human factor.

Finally, the spyware implemented in this paper will not detect any forbidden acts, if the e-exam system run in a virtual machine; therefore, it is recommended that further research in this direction should incorporate virtual machine detection mechanism.

## 8. REFERENCES

[1] Al-Hakeem, M. S. & Abdulrahman, M.S (2017). Developing a New e-Exam Platform to Enhance the University Academic Examinations: the Case of Lebanese French University, International .Journal of Modern Education and Computer Science, 5(1), 9-16

[2] Ann, B., & Kannammal, A. (2014). Information Security Modelling in An E-learning Environment. International Journal of Computer Science, 11(1), 23 - 29.

[3] Alwi, N.H.M., & Fan, I. (2010). E-Learning and Information Security Management, International Journal of Digital Society (IJDS), 1(2), 148-156

[4] Baller, M., Lukandu, A. & Radwan, A. (2015). Improving Learning Throughput in E-learning using Interactive-Cognitive Based Assessment. The International Journal of E-learning and Educational Technologies in the Digital Media (IJEETDM) 1(1);

32-49.

[5] Baller, M., Lukandu, A. & Radwan, A. (2015). Reversed Roulette Wheel Selection Algorithms (RWSA) and Reinforcement Learning (RL) for Personalizing and Improving E-learning System: The case study and its implementation. The International Journal of E-learning and Educational Technologies in the Digital Media (IJEETDM) 1(2); 92-108.

[6] Bobde, S., Chaudhari, S. Golguri, J. & Shahane, R. (2017). Web Based Online Examination System, Global Research and Development Journal for Engineering, 2(5), 58- 61

[7] Farid, S. Alam, M., XQaiser, M., Haq, A. A. U. & Itmazi, J. (2017). Security Threats and Measures in E-learning in Pakistan: A Review, Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan, 22(3), 98-107.

[8] Frank, A. J. (2010). Dependable Distributed Testing – Can the Online Proctor be reliably computerized. In: Proc. International Conference on e-Business (ICE-B), Athens.

[9] Furnell, S. M., & Karweni, T. (2001). Security issues in Online Distance Learning, VINE. The Journal of Information and Knowledge Management Systems, 31(2), 28- 35

[10] Ismail, H. M. & Soye, M. (2018). Biometric Enabled Computer-Based Testing System (CBT) With Advanced Encryption Standard (AES), Journal of Emerging Technologies and Innovative Research, 5(8),579- 585

[11] Jegatha D. L., Karthika, R., Vijayakumar, P., Rawal, B.S. & Wang, Y. (n.d).Secure Online Examination System for e-learning

[12] Kitahara, R., Westfall, F., & Mankelwicz, J. (2011). New, multi-faceted hybrid approaches to ensuring academic integrity. Journal of Academic and Business Ethics, 3(1), 1–12.

[13] Maity,P., Patil, S., Pednekar,P. , Sawant4, A. & Rupnar, M. (2018). Online Examination System, International Research Journal of Engineering and Technology (IRJET), 5(3), 1956 – 1957

[14] Meletiou, G.I., Voyiatzis, V. & Sgouropoulou, C. (2012). Design and Implementation of an e-exam system based on the Android platform, In: Proc. 16th Panhellenic Conference on Informatics.

[15] Naveen, J. M., Kumar, G. P. Mukhilan, V, Manoj Prasad, T Ramasamy, & Harini N. (2018). Multi-factor authentication scheme for online examination, International Journal of Pure and Applied Mathematics, 119(15), 1705-1712

[16] Osang, F. (2012). Electronic Examination in Nigeria, Academic Staff Perspective—Case Study: National Open University of Nigeria (NOUN). International Journal of Information and Education Technology, 2(4), 304 – 307.

[17] Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber-attacks and novice IT management in a small university. Journal of Cases on Information Technology, 8(4), 24-34.

[18] Sarjiyus, O. (2019). Securing Computer Based Testing (CBT) System for Tertiary Institutions in Nigeria Asian Journal of Research in Computer Science, 3(3): 1-16.

[19] Singh, U. G. (2015). Solving the 'Riddel' of e-Assessment: Student perceptions. The International Journal of E-learning and Educational Technologies in the Digital Media (IJEETDM), 1(3); 142-153.

[20] Swathi P. S., Narayanan, A. & Bijlani, K. (2016). "An Intelligent System for Online Exam Monitoring" in Information Science (ICIS), International Conference, 2016

[21] Traoré, I., Nakkabi, Y. , Saad, S. Sayed, B., J.D. Ardigo & de Faria Quinan, P.M. (2017). Ensuring Online Exam Integrity Through Continuous Biometric Authentication, Information Security Practices, Springer International Publishing, DOI 10.1007/978-3-319-48947-6_6, 73 – 81.

[22] Treenantharath, T., & Sutheebanjard, P. (2013). Secure Online Exams on Thin Client. In: Proc. 11th International Conference on ICT and Knowledge Engineering (ICT&KE).

[23] Ullah, A., Xiao, H. & Barker, T. (2019). A study into the usability and security implications of text and image based challenge questions in the context of online examination, Educational Informational Technology, 24(1),:13–39.

[24] Wong, T.-K., Xie, H., Zou, D., Wang, F. L., Tai Tang, J. K., & Kong, A.(2019). How to facilitate self-regulated learning? A case study on open educational resources. Journal of Computers in Education. https://doi.org/10.1007/s40692-019-00138-4.

[25] Zhang, J., Zhao, L. & Nunamaker, J. F. (2004): Can e-learning replace classroom learning? Communications of the ACM, 47(5): 75-